(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 880 088 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
25.11.1998 Bulletin 1998/48

(51) Int. Cl.[6]: **G06F 1/00**

(21) Application number: **98109085.5**

(22) Date of filing: **19.05.1998**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **23.05.1997 JP 149999/97**

(71) Applicant:
MITSUBISHI CORPORATION
Chiyoda-ku Tokyo 100 (JP)

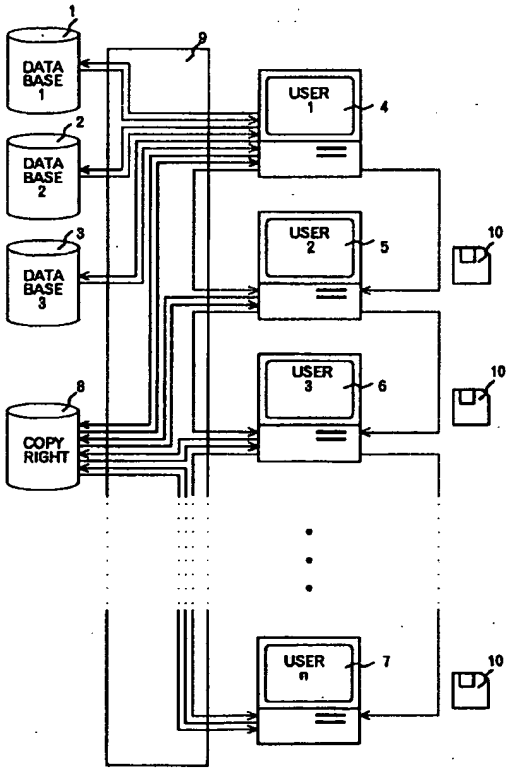
(72) Inventor: **Saito, Makoto**
Tama-shi (JP)

(74) Representative:
Neidl-Stippler, Cornelia, Dr.
Rauchstrasse 2
81679 München (DE)

(54) Data copyright management system and apparatus

(57) There are provided a digital content management apparatus which further embodies a digital content management apparatus used with a user terminal, and a system which protects the secrets of a digital content. The system and the apparatus are a real time operating system using a micro-kernel, which is incorporated in the digital content management apparatus as an interruption process having high priority, or is arranged in a network system using the digital content. When a user uses the digital content, whether there is an illegitimate usage or not, is watched by interrupting the usage process. In the case where illegitimate usage is carried out, a warning is given or the usage is stopped. The decryption/re-encryption functions of the digital content management apparatus having the decryption/re-encryption functions are not restricted to the inside of the user apparatus. By providing the decryption/re-encryption functions between the networks, the exchange of secret information between different networks is secured. By using this apparatus for converting a crypt algorithm, information exchange is made possible between systems which adopt different algorithms.

Fig. 1



EP 0 880 088 A2

Description

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to a system for managing digital content, specifically for managing a copyright of digital content claiming the copyright and for securing secrecy of digital content, and also relates to an apparatus implementing this system.

Background Art

In information- oriented society of today, a database system has been spread in which various data values having been stored independently in each computer so far are mutually used by connecting computers by communication lines.

The information having been handled so far by the database system is classical type coded information which can be processed by a computer and has a small amount of information or monochrome binary data like facsimile data at most. Therefore, the database system has not been able to handle data with an extremely large amount of information such as a natural picture and a motion picture.

However, while the digital processing technique for various electric signals develops, development of the digital processing art has shown progress for a picture signal other than binary data having been handled only as an analog signal.

By digitizing the above picture signal, a picture signal such as a television signal can be handled by a computer. Therefore, a "multimedia system" for handling various data handled by a computer and picture data obtained by digitizing a picture signal at the same time is noticed as a future technique.

Because hitherto widely-spread analog content is deteriorated in quality whenever storing, copying, editing, or transmitting it, copyright issues associated with the above operations have not been a large problem. However, because digital content is not deteriorated in quality after repeatedly storing, copying, editing, or transmitting it, the control of copyrights associated with the above operations is a large problem.

Because there is not hitherto any exact method for handling a copyright for digital content, the copyright is handled by the copyright law or relevant contracts. Even in the copyright law, compensation money for a digital-type sound-or picture- recorder is only systematized.

Use of a database includes not only referring to the contents of the database but also normally effectively using the database by storing, copying, or editing obtained digital content. Moreover, it is possible to transmit edited digital content to another person via on-line by a communication line or via off-line by a proper recording medium. Furthermore, it is possible to transmit the edited digital content to the database to enter it as new digital content.

In an existing database system, only character data is handled. In a multimedia system, however, audio data and picture data which are originally analog content are digitized to a digital content and formed into a database in addition to the data such as characters which have been formed into a database so far.

Under the above situation, how to handle a copyright of digital content formed into a database is a large problem. However, there has not been adequate copyright management means for solving the problem so far, particularly copyright management means completed for secondary utilization of the digital content such as copying, editing, or transmitting of the digital content.

Although digital content referred to as software with advertisement or as freeware is, generally, available free of charge, it is copyrighted and its use may be restricted by the copyright depending on the way of use.

In view of the above, the inventor of the present invention has made various proposals thus far in order to protect a copyright of the digital content. In GB 2269302 and U. S. Patent 5,504,933, the inventor has proposed a system for executing copyright management by obtaining a permit key from a key management center through a public telephone line, and has also proposed an apparatus for that purpose in GB 2272822. Furthermore, in EP 677949 and in EP 704785, a system has been proposed for managing the copyright of the digital content.

In these systems and apparatus, those who wish to view encrypted programs request to view a program uing a communication device to a management center via a communication line, and the management center transmits a permit key in response to the request for viewing, and charges and collects a fee.

Upon receipt of the permit key, those who wish to view the program send the permit key to a receiver either by an on-line or an off-line means and the receiver, which has received the permit key, decrypts the encrypted program according to the permit key.

The system described in EP 677949 uses a program and copyright information to manage a copyright in addition to a key for permitting usage in order to execute the management of the copyright in displaying (including process to sound), storing, copying, editing, and transmitting of the digital content in a database system, including the real time transmission of digital picture content. The digital content management program for managing the copyright watches and manages to prevent from using the the digital content outside the conditions of the user's request or permission.

Furthermore, EP 677949 discloses that the digital content is supplied from a database in an encrypted state, and is decrypted only when displayed and edited by the digital content management program, while the digital content is encrypted again when stored, copied or transmitted. It is also described that the digital con-

tent management program itself is encrypted and is decrypted by the permit key, and that the decrypted digital content management program performs decryption and encryption of the digital content, and when usage other than storing and displaying of the digital content is executed, the copyright information is stored as a history, in addition to the original copyright information.

In U. S. Patent Application No.08/549,270 and EP 0715241 relating to the present application, there is proposed an apparatus for decryption/re-encryption having configuration of a board, PCMCIA card or an IC card for managing the copyright, and a system for depositing a crypt key. Also, a reference is made to apply the copyright management method to a video conference system and an electronic commerce system.

In U.S. Patent Application No.08/549,271 and EP 709760, a system has been proposed wherein the protection of an original digital content copyright and an edited digital content copyright in case of the edited digital content using a plurality of digital contents is carried out by confirming the validity of a usage rquest according to a digital signature on an edit program by combining a secret-key cryptosystem and a public- key cryptosystem.

In U.S. Patent Application No.08/573,958 and EP 719045, various forms have been proposed for applying the digital content management system to database and video-on-demand (VOD) systems or an electronic commerce.

In U.S. Patent Application No.08/663,463, EP 746126, a system has been proposed, in which copyrights on an original digital content and a new digital content are protected by using a third crypt key and a copyright label in case of using and editing a plurality of digital contents.

As can be understood from the digital content management systems and the digital content management apparatus which have been proposed by the inventor of the present invention, described above, the management of a digital content copyright can be realized by restricting encryption/decryption/re-encryption and the form of the usage by using the copyright management program. The cryptography technology and the usage restriction thereof can be realized by using a computer.

In order to use the computer efficiently, an operating system (OS) is used which, supervises the overall operation of the computer. The conventional operating system used on a personal computer or the like is constituted of a kernel for handling basic services such as memory control, task control, interruption, and communication between processes and OS services for handling other services.

However, improvement in the functions of the OS which supervises the overall operation of computers is now being demanded where circumstances change on the computer side, such as improved capability of microprocessors, a decreased price of RAM (Random Access Memory) used as a main memory, as well as improvement in the performance capability of computers is required by users, as a consequence, the scale of an OS has become comperatively larger then before.

Since such an enlarged OS occupies a large space itself in the hard disk stored OS, the space for storing the application programs or data needed by the user is liable to be insufficient, with the result in which the usage convenience in the computer becomes unfavorable.

In order to cope with such a situation, in the latest OS, an environmental sub- system for performing emulation of other OS and graphics displaying, and a core sub- system such as a security sub-system are removed from the kernel, as a sub- system that is a part that depends on the user. The basic parts such as a HAL (hardware abstraction layer) for absorbing differences in hardware, a scheduling function, an interruption function, and an I/O control function is a micro-kernel, and a system service API (Application Programming Interface) is interposed between the sub- system and the micro- kernel, thereby constituting the OS.

By doing so, extension of the OS by change or addition of functions will be improved, and portability of the OS can be facilitated corresponding to the applications. By a distributed arrangement for elements of the micro-kernel to a plurality of network computers, the distributed OS can also be realized without difficulty.

Computers are used in computer peripheral units, various control units, and communication devices in addition to the personal computers represented by the desktop type or notebook type computers. In such a case, as an OS unique for embedding, applicable to each of the devices, a real time OS is adopted in which execution speed is emphasized, unlike a general-purpose personal computer OS, in which the man-machine interface is emphasized.

Naturally, the development cost for a respective OS unique to each device embedded will be high. There has recently been proposed, therefore, that a general-purpose OS for personal computers as a real-time OS for embedding is used instead. By arranging a specified program for embedding in a sub- system combined with the micro-kernel, a real-time OS for embedding can be obtained.

As the major functions of an OS, there is a task control, such as scheduling, interruption processing, and the like. With respect to task control, there are two kinds of OS's; the single-task type, in which only one task is executed at the same time, and the multi-task type, in which a plurality of task processes are executed at the same time. The multi-task type is further classified into two kinds; one multi-task type, changing of tasks depends on the task to be executed, and the other multi-task type, the changing does not depend on the task to be executed.

In the aforementioned types, the single-task type assignes one process to a CPU (central processing unit) and the CPU is not released until the process

comes to an end, and a non-preemptive multi-task type performs time-division for the CPU, and the CPU can be assigned to a plurality of processes. As long as the process which is being executed does not give control back to the OS, other processes are not executed. And a preemptive multi-task type interrupts the process which is being executed during a certain time interval and thereby forcibly move the control to another process. Consequently, real time multi-task can be available only in the case of the preemptive type.

Task control in a computer is performed according to processes being units having system resources such as a memory and a file. Process control is performed according to a thread, being a unit in which CPU time is assigned, in which the process is minutely divided. Incidentally, in this case, the system resources are shared in all the threads in the same process. More than one threads, therefore, may exist which share the system resources in one process.

Each task which is processed by the multi- task type has a priority spectrum, which is generally divided into 32 classes. In such a case, a normal task without interruption is classified into dynamic classes which are divided into 0 to 15 classes, while a task performing interruption is classified into real- time classes divided into 16 to 31 classes.

Interruption processing is carried out using interruption enabling time (generally, 10ms) referred to as a time slice, as one unit. A normal interruption is carried out during a time slice of 10ms. In such a situation, a time slice has recently been proposed wherein the interruption enabling time is set to 100 μs. When such a real time slice is used, an interruption can be carried out with greater priority than the conventional 10 ms.

SUMMARY OF THE INVENTION

In the present application, there is proposed a digital content management apparatus which farther embodies a digital content management apparatus which can be used with the user terminal proposed in EP 704785, for managing a digital content, specifically, a copyright of the digital content claiming the copyright. And also there is proposed a system to which the idea applied to the digital content management apparatus is further applied for secrecy protection of the digital content.

In the present application, a system for watching the illegitimate usage of the digital content and an apparatus therefor are proposed. These system and apparatus are a real time operating system using a microkernel, and are incorporated in the digital content management apparatus as an interruption process having a high priority, or are arranged in a network system using the digital content It is watched whether an illegitimate usage or not, by interrupting into the use process when a user utilizes the digital content In the case where illegitimate usage is performed, a warning or a stop for the usage is given.

Furthermore, in the present application, decryption/re-encryption functions in the digital content management apparatus having the decryption/re-encryption functions are not restricted within the user apparatus but are provided in a gateway or a node between the networks, so that the exchange of secret information is secured between different networks.

By using the apparatus according to the present invention, for the conversion of crypt algorithm, information exchange can be made possible between systems which adopt different crypt algorithms.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a structural view of a digital content management system to which the present invention is applied.

Figure 2 is a structural view of a digital content management apparatus to which the present invention is applied.

Figure 3 is a structural view of another digital content management apparatus to which the present invention is applied.

Figure 4 is a structural view of a system for watching the digital content usage according to the present invention.

Figure 5 is a structural view of a system for protecting digital content secrecy according to the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The description of the preferred embodiments according to the present invention is given below referring to the accompanied drawings.

Figure 1 shows a structure of the digital content management system to which the present application applies.

In this digital content management system illustrated in Figure 1, reference numerals 1, 2 and 3 represent databases stored text data, binary data of a computer graphhics screen or a computer program and digital content of sound or picture data, which are not encrypted. 9 represents a communication network constituted of using a public telephone line offered by a communication enterprise or a CATV line offered by a cable television enterprise, 4 represents a primary user terminal, 5 represents a secondary user terminal, 6 represents a tertiary user terminal, and 7 represents an n-order user terminal, and 8 represents a digital content management center.

On the above arrangement, the databases 1, 2, 3, the digital content management center 8, primary user terminal 4, secondary user terminal 5, tertiary user terminal 6, and n-order user terminal 7 are connected to the communication network 9.

In this figure, a path shown by a broken line repre-

sents a path for transferring encrypted digital content, a path shown by a solid line represents a path for transferring requests from each of the user terminals 4, 5, 6, 7 to the digital content management center 8 and databases 1, 2, 3, a path shown by a one-dot chain line represents a path through which a permit key corresponding to a usage request, a digital content management program and a crypt key are transferred from each of the databases 1, 2, 3, and the digital content management center 8 to each of the user terminals 4, 5, 6, 7.

This digital content management system employs a first public-key Kb1, a first private-key Kv1 corresponding to the first public-key Kb1, a second public-key Kb2, and a second private-key Kv2 corresponding to the second public-key Kb2 that are prepared by the user, and a first secret-key Ks1 and a second secret-key Ks2 prepared by the database. The database encrypts digital content M by using the first secret-key Ks1:

$$Cmks1 = E(Ks1, M),$$

and further encrypts the first secret-key Ks1 by the first public-key Kb1:

$$Cks1kb1 = E(Kb1, Ks1)$$

and the second secret-key Ks2 by the second public-key Kb2:

$$Cks2kb2 = E(Kb2, Ks2).$$

The database then transfers these encrypted digital content Cmks1, the first and the second secret-keys Cks1kb1 and Ck2kb2 to the user.

The user decrypts the encrypted first secret-key Cks1kb1 using the first private- key Kv1:

$$Ks1 = D(Kv1, Cks1kb1),$$

and decrypts the encrypted digital content Cmks1 by the decrypted first secret-key Ks1:

$$M = D(Ks1, Cmks1)$$

and uses it. The user decrypts encrypted second secret-key Cks2kb2 by the second private-key Kv2:

$$Ks2 = D(Kv2, Cks2kb2),$$

which is subsequently used after decryption as a crypt key for storing, copying, or transferring digital content.

If the primary user 4 copies digital content obtained and then supplies it to the secondary user 5, the digital content does not involve the copyright of the primary user 4 because no modifications have been made to the digital content. If, however, the primary user 4 produces new digital content based on the digital content obtained or using a means for combining with other digital content, the new digital content involves a secondary copyright for the primary user 4, and the primary user 4 has the original copyright for this secondary work.

Similarly, if the secondary user 5 produces further new digital content based on the digital content obtained from the primary user 4 or using a means of combining with other digital content, the new digital content involves a secondary copyright for the secondary user 5, and the secondary user 5 has the original copyright of this secondary work.

Databases 1, 2, and 3 store text data, binary data constituting computer graphics screens or programs and digital content such as digital audio data and digital picture data, which are to be encrypted and supplied to the primary user terminal 4 via network 9 during a digital content read operation in response to a request from the primary user terminal 4.

Managing the digital content obtaining from the database is carried out by the method described in Japanese Patent Laid-open No.185448/1996 or in Japanese Patent Laid- Open No.287014/1996, which have been proposed by the present inventor.

Recently, a PCI (Peripheral Component Interconnect) bus has attracted attention as means for implementing a multiprocessor configuration in a typical personal computer. The PCI bus is a bus for external connection connected to a system bus of a computer via a PCI bridge, and allows to implement a multiprocessor configuration.

The digital content includes graphics data, computer programs, digital audio data, still picture data by JPEG and also moving picture data by MPEG 1 or MPEG 2, in addition to character data. In case that the digital content to be managed is moving picture data by JPEG still picture system or moving picture data by MPEG 1 or MPEG 2, as having remarkably large amount of data with high speed, managing the digital content by a single processor is difficult.

Figure 2 is a block diagram illustrating an arrangement of a digital content management apparatus used for managing the digital content of the above in the digital content management system shown in Figure 1.

The digital content management apparatus comprises a first digital content management apparatus 12 connected to a user terminal 11 and a second digital content management apparatus 13.

The first digital content management apparatus 12 has a computer configuration having a MPU (Micro-Processor Unit) 24, a local bus 25 of MPU 24, ROM (Read-Only Memory) 26 connected to the local bus 25, RAM 27 and EEPROM (Electrically Erasable Programmable Read-Only Memory) 31.

A PCI bus 23 is connected to a system bus 15 for a microprocessor 14 of the user terminal 11 via a PCI bridge 22 and the local bus 25 for the MPU 24 of the digital content management apparatus 12, and also a local

bus 30 for MPU 29 of the digital content management apparatus 13 are connected to the PCI bus 23. Also connected to the system bus 15 of the user terminal 11 are a communications device (COMM) 21 which receives digital content from external databases and transfers digital content to the external of the terminal, a CD-ROM drive (CDRD) 20 which reads digital content supplied on CD-ROM, a flexible disk drive (FDD) 19 which copies received or edited digital content in a flexible disk to supply to the external of terminal, and hard disk drive (HDD) 18 used for storing digital content. COMM 21, CDRD 20, FDD 19, and HDD 18 may also be connected to the PCI bus 23. While ROM, RAM etc., of course, are connected to the system bus 15 of the user terminal, these are not shown in Figure 2.

The decryption and re-encryption operations are performed by either of the MPU 24 of the first digital content management apparatus 12 and the MPU 29 of the second digital content management apparatus 13, i.e., one performs decryption and the other performs re-encryption at the same time. Since the configuration of the MPU 24 and MPU 29 in Figure 2 is a multiprosessor configuration which performs parallel processing with a PCI bus 23, high processing speed can be achieved.

In the digital content management apparatus shown in Figure 2, the storage device, such as HDD 18, for storing re-encrypted digital content is connected to the system bus 15 of the user terminal 11. In order to store re-encrypted digital content, therefore, the encrypted digital content must be transferred by way of the system bus 15 of the user terminal 11 and the local bus 25 or 30 of the digital content management apparatus 12 or 13, and consequently, processing speed can be slowed.

In the digital content management apparatus shown in Figure 3, a communications device COMM and a CD-ROM drive CDRD are connected to a local bus of a digital content management apparatus for decryption, and a storage device such as HDD for storing re-encrypted digital content is connected to the local bus of a digital content management apparatus for re-encryption.

The digital content management apparatus 35 for decryption has the computer system configuration having a MPU 37, a local bus 38 for the MPU 37, and ROM 39, RAM 40 and EEPROM 41 connected to the local bus 38, and a communication device COMM 42 and a CD-ROM drive CDRD 43 are connected to the local bus 38. The encrypted digital content supplied from the communication device COMM 42 and the CD-ROM drive CDRD 43 is decrypted in this apparatus.

The digital content management apparatus 36 for re- encryption has the computer system configuration having a MPU 44, a local bus 45 for the MPU 44, and ROM 46, RAM 47 and EEPROM 48 connected to the local bus 45, and HDD 39 is connected to the local bus 45. The digital content which has been re-encrypted in the digital content management apparatus 36 for re-encryption is stored in HDD 39.

In the protection of a digital content copyright, the greatest issue is how to prevent from illegitimate usage of the digital content on the user side apparatus. Decryption/re-encryption and restriction on usage are carried out by a digital content management program for this purpose.

However, since decryption/re-encryption of the digital content to be protected the copyright is performed using an apparatus on the user side, it is virtually impossible to expect that processing of the decryption/re-encryption and the management of the crypt key which is used for the purpose will be complete. There is a possibility that the digital content will be illegitimately stored, copied, transmitted and edited by invalidating the digital content management program.

In order to restrict such illegitimate usage, it is required that a digital content management program for decryption/re-encryption of the digital content, and for managing the crypt key cannot be altered by the user. For this purpose, incorporation of the digital content management program into the hardware is the most secure method.

For example, there is a configuration in which a dedicated scramble decoder is currently used for descrambling scrambled broadcast programs in analog television broadcast, so that decryption/re-encryption of the digital content and management of the crypt key are available only by using a dedicated digital content management apparatus.

Although such a configuration is reliable, the system structure is lacking in flexibility. When the apparatus on the user side is changed, or the digital content management program is changed, it is very hard for the user to respond to such changes. In case of a network computer on which has been recently focused, since the network computer does not have a function for storing the digital content management program, it would be impossible to realize the digital content management program in the hardware.

In order to correspond with flexibility to a case where the apparatus on the user side changes, or a case where the digital content management program is changed, it is desirable for the digital content management program to be software. However, there is a possibility that the digital content management program is altered as long as the digital content management program is an application program.

For the digital content management program being software, the digital content management program is required to be incorporated in a kernel that is a fixed area in OS and cannot be altered by the user. However, it is not practical for the digital content management program to be incorporated in the fixed area of the kernel, where the digital content management system and the cryptosystem are differentiated between the databases.

As described above, some real time OS can perform interruption in real time slice time which is one or

two figures faster than the time slice of the system in another OS that includes kernel area. By using this technology, the usage status of the digital content which is claiming the copyright, is watched without affecting the overall operation. And if an illegitimate usage is found, it is possible to give a warning or to forcibly stop the usage thereof.

Next, a method for reinforcing a digital content management program by using a real time OS is described.

The digital content management apparatus shown in Figure 2 has a multi- processor structure in which a first digital content management apparatus 12 and a second digital content management apparatus 13 are connected to an apparatus on the user side via a PCI bus. The decryption operation of the first digital content management apparatus 12 and re-encryption operation of the second digital content management apparatus 13 are controlled by the digital content management program in the user terminal 11.

The digital content management program of the user terminal 11 also manages the operations of the communication device 21, the CD-ROM drive 20, the flexible disk drive 19 and the hard disk drive 18, which manages loading or downloading of encrypted digital content, and storing into the hard disk drive 18, copying to the flexible disk drive 19 and uploading to the communication device 21 of re-encrypted digital content.

Since illegitimate usage of the digital content is carried out by unauthorized editing, unauthorized storing, unauhorized copying or unauthorized uploading of the decrypted digital content, whther the illegitimate usage has been carried out or not, can be detected by whether editing, storing, copying or uploading of the decrypted digital content is performed or not. As a consequence, the process for watching the illegitimate usage interrupts a digital content use process which is being executed in a certain time interval, while interrupting by a preemptive type multi-task which forcibly carries out watching of the process.

The multi-task time slice normally carried out is 10ms, and the decryption/re-encryption process is carried out in this time unit. On the other hand, the fastest real time slice is 100 μs, which is 1/100 of the normal time unit. Consequently, the watching task, which has high interruption priority, can watch the digital content as to whether the decrypted digital content is being edited, stored, copied or uploaded, so that the usage status of the digital content for which the copyright is claimed can be watched without affecting regular usage by the user, and the illegitimate usage is found, a warning can be given and usage thereof can be forcibly stopped.

The digital content management program with such a watching function is incorporated into a sub- system area which is operated in the user mode in place of the kernel of the OS, and the watching process is regarded as a process with a high priority. By constituting the system in this way, the usage status of the digital content by decryption/re-encryption and also the illegitimate usage other than the permitted usage can be watched at the same time, and such watching can be executed smoothly.

Since these operations are the same in the case of the digital content management apparatus which is shown in Figure 3, a further explanation thereof is omitted.

Next, a structure for watching the illegitimate usage of the digital content in the distributed OS is described referring to Figure 4. Figure 4 illustrates a structure of a general distributed type OS, in which servers 51 to 54 and clients 55 to 58 are connected to a network 50.

The network 50 is a restricted network such as LAN (Local Area Network) in a office. Each of the servers 51 to 54 stores basic OS elements of the micro-kernel, application elements which are a sub-system, or the digital content. In order to manage the digital content, the digital content management program which has been described so far is required. This digital content management program is stored, for example, in the server 54. And the watching program for watching the illegitimate usage of the digital content having a high priority for interruption is stored, for example, in the supervisory server 51 for supervising the overall operation of the distributed OS.

Although the terminal apparatus of the clients 55 to 58 is a simple terminal, the terminal is provided with a copying device such as a flexible drive or the like when necessary.

In such a structure, when the clients 55 to 58 use the digital content which is stored in the servers 51 to 54, the clients 55 to 58 are supplied the micro-kernel that is the basic OS elements from each of the servers, and also supplied the digital content management program which is stored in the server 54, and thus, the digital content can be used.

The digital contents stored in the server are either encrypted or not encrypted. In either of these cases, the digital content is supplied with encrypted when supplied to the clients. Therefore, in order for the client to use the encrypted digital content, it is necessary to obtain the crypt key and to decrypt by the digital content management program as has been described above.

The fact that the client uses the digital content and the digital content management program is grasped by the supervisory server 51. This watching process automatically interrupts the process which is being executed by the client at regular intervals without the client's request, and watchs, and gives a warning or stop of the usage if an illegitimate usage is detected.

Since such a watching process can be completed with a process having a small size, and therefore, that affects little on the operation on the client side, and the user does not notice the operation of the watching program.

In the distributed OS, the servers and the clients have been explained as separated. However, the afore-

mentioned structure may be applied when a client machine is provided with a hard disk drive, and the client machine also serves as the server machine. When the network 50 is not a restricted one as LAN in a office, but a non- restricted one such as the Internet system, the aforementioned structure can be also applied.

In particular, such a structure is effective in a network computer system. Even in the case where the user modifies a computer not provided with a storage device, a copying device or a communication device for transmission, or use a normal computer pretending to be of a network computer system, the digital content can be managed by remote control.

Furthermore, the structure can be applied to the digital content management system shown in Figure 1. In such a case, the watching program is stored in the digital content management center 8 of Figure 1 to regularly watch whether users illegitimately use the encrypted digital content supplied from the database through the network 9 by remote control.

In case that the digital content is broadcast via analog data broadcast or via digital data broadcast, the watch program may be transferred by inserting to the digital content. Also, the watch program may be resident in a apparatus of the digital content user so that the remote control is made possible by periodically broadcasting watch program control signal.

In the case where the digital content having a large amount of information, such as digital picture content is handled in the digital content management system which is carried out via the network, an ISDN (Integrated System for Digital Network) line is used in many cases as a communication line.

As the ISDN line, there are generally used two data channels having data transmission speed of 64 Kbps (kilo bits per second) referred to as B cannels, and a control channel having data transmission speed of 16 Kbps referred to as D channel. Naturally, the digital content is transmitted through one or two data channels, while the D channel is not used in many cases.

Thus, if the D channel is used for the interrupting watching by the watch program, it would be possible to watch the usage status by remote control without affectioning the usage of the digital content at all.

When the user uses information to which a copyright is claimed, the real time OS is automatically linked to the key center, it is also possible to watch and manage the re-encryption mechanism with a real time OS as a result.

Further, in the case where a digital content creator or an end user uses information to which a copyright is claimed, a re-encryption program resident in the PC uses the real time OS so that remote watching and managing can be made possible.

Next, application of the digital content management system to the prevention of the leakage of information is described. Figure 5 illustrates a structure of the system for preventing from the leakage of information by applying the system to an intranet system in which a LAN is connected to the Internet system.

In Figure 5, reference numerals 60, 61, and 62 represent the network systems which are connected to each other by a public lines 63, 63. In particular, the network system 62 is a LAN system established in a office or the like. These network systems are connected with each other via a public communication line or the like to constitute an Internet system as a whole. Clients 64, 64, 64 are connected to the LAN system 62 and servers not shown in the figure are connected in addition.

The LAN system has secret data such as business secrets and the like therein. Since the LAN system is connected to the outside network, the problems of the leakage of the secret information to the outside, or of the access to the secret information from the outside may arise. As a consequence, although an information partition, called a "fire-wall," is normally provided between the LAN system and the public line, that is not technologically perfect. Also, even in the case of the business secret data, it may be necessary to supply the business secret data to another party, where the another party network has a common interest, and in such a case, the presence of the fire-wall becomes an obstacle.

As has been described repeatedly, the management of the secret data can be completely carried out through encryption. In the case where the crypt algorithm used in the other party network is common with the algorithm used in the one's own network, the secret data can be shared by sending the crypt key to the other party by some means. In the case where the crypt algorithm used in the other party network is different from the algorithm which is used in one's own network, such means cannot be adopted.

In order to cope with such a problem, crypt key conversion devices 65, 66 and 67 are arranged in place of or together with the fire-wall in the Internet system shown in Figure 5. These crypt key conversion devices 65, 66 and 67 have the same configuration as the digital content management apparatus which have been described by using Figures 2 and 3, and perform decryption/re-encryption by two different crypt keys.

For example, the crypt algorithm conversion device 65 decrypts the data which is encrypted by a crypt algorithm unique to the network 60 and re-encrypts the decrypted data by a crypt algorithm which is common in the whole Internet system. The crypt algorithm conversion device 67 that has received the re-encrypted data decrypts the re-encrypted data, encrypts the decrypted data by the crypt algorithm unique to the network 62, and supplies it to the client 64.

By doing so, it becomes possible to handle the encrypted data between networks that adopt different crypt algorithms. Here, there may be two cases; one is a case in which the crypt key is not changed at all, and the other is a case in which the crypt key is changed at each stage.

In using databases, in a case where a data storing server referred to as "proxy server" or "chache server" is used, and where the digital content is encrypted, the crypt key or crypt algorithm used between the data server and the proxy server may be diffrentiated from the crypt key or crypt algorithm used between the proxy server and a user, and then, the conversion of them is carried out by using the crypt key conversion device or crypt algorithm conversion device, so that the encrypted digital content can be prevented from illegitimate usage thereof.

The conversion of the crypt algorithm by these devices can be effected by units of countries. Even in the case where crypt algorithms are used which differ from one country to another, it becomes possible to adopt a key escrow system unique to the respective country, or a key recovery system using the key escrow system.

For example, the crypt key conversion device 65 decrypts an encrypted data from the network 60, and re-encrypts the decrypted data by using the crypt key common to the whole Internet system. The crypt key conversion device 67 which has received the re-encrypted data decrypts the re-encrypted data by using the crypt key common to the whole Internet system, and re-encrypts the decrypted data and supplies it to the client 64. By doing this, the problem of sending the crypt key is alleviated.

These crypt key conversion devices 65, 66 and 67 can be arranged in a gateway or a node which is used as a connection between networks. Further, even in a closed network system other than the Internet, which is a liberated system, this system functions efficiently in such cases where individual information such as reliability information, medical information or the like is handled, and where access to the data is necessary to differ by levels.

These crypt key conversion devices also can be used so as to convert the crypt algorithm. There are plurality of crypt algorithms which are currently used or proposed. In the worst case, a plurality of networks using different crypt algorithms respectively coexist, and thus, compatibility is lost, which becomes an obstacle to the development of the information oriented society. Even if a new effective crypt algorithm is developed, and if it has not compatibility with the existing crypt algorithm, an obstacle to the development of the information oriented society may similarly be brought.

In order to cope with such problems, the crypt algorithm can be converted by arranging the crypt key conversion devices 65, 66 and 67 of Figure 5 in the gateway or in the node. These crypt algorithm conversion devices decrypt the encrypted data to be re-encrypted with a different crypt algorithm.

Claims

1. A digital content management system which uses a digital content, for managing digital content copyrights having:

   a server in which a watch program with high interruption priority is stored, and being constituted as a real time operating system using a micro-kernel, in a network.

2. A digital content management apparatus used via a user terminal which uses a digital content, for managing digital content copyrights, comprising:

   said digital content management apparatus comprising a microprocessor, a microprocessor bus, a read-only semiconductor memory, an electrically erasable and programmable read-only memory, and a read/write memory, wherein:

   said microprocessor, said read-only semiconductor memory, said electrically erasable and programmable read-only memory and said read/write memory are connected to said microprocessor bus, and a system bus of said user terminal is capable of being connected to said microprocessor bus;

   a digital content management system program, a crypt algorithm, and a watch program which is a micro-kernel type real time operating system are stored in said read-only semiconductor memory; and

   a first public-key, a first private-key, a second public-key, a second private-key, a digital content management program, a first secret-key, a second secret key and copyright information are stored in said electronically erasable and programmable read-only memory.

3. A digital content management system which protects the secrets of a digital content in a network having a decryption/re-encryption apparatus between networks.

4. A digital content management apparatus which protects the secrets of a digital content in a network comprising:

   said digital content management apparatus comprising a microprocessor, a microprocessor bus, a read-only semiconductor memory, an electrically erasable and programmable read-only memory and a read/write memory, wherein

   said microprocessor, said read-only semiconductor memory, said electrically erasable and

programmable read-only memory and said read/write memory are connected to said microprocessor bus, and a system bus of the user terminal is capable of being connected to said microprocessor bus;

a digital content management system program, a crypt algorithm, and a watching program which is a micro-kernel type real time operating system are stored in said read-only semiconductor memory; and

a first public-key, a first private-key, a second public-key, a second private-key, a digital content management program and a first secret-key, a second secret-key, and copyright information are stored in said electrically erasable and programmable read-only memory.

5. A digital content management apparatus according to claim 2 or 4, which is configured in the form of an IC chip.

6. A digital content management apparatus according to claim 2 or 4. which is configured in the form of an IC card.

7. A digital contents management apparatus according to claim 2 or 4, which is configured in the form of a PC card.

8. A digital contents management apparatus according to claim 2 or 4, which is configured in the form of an inserted board.

Fig. 1

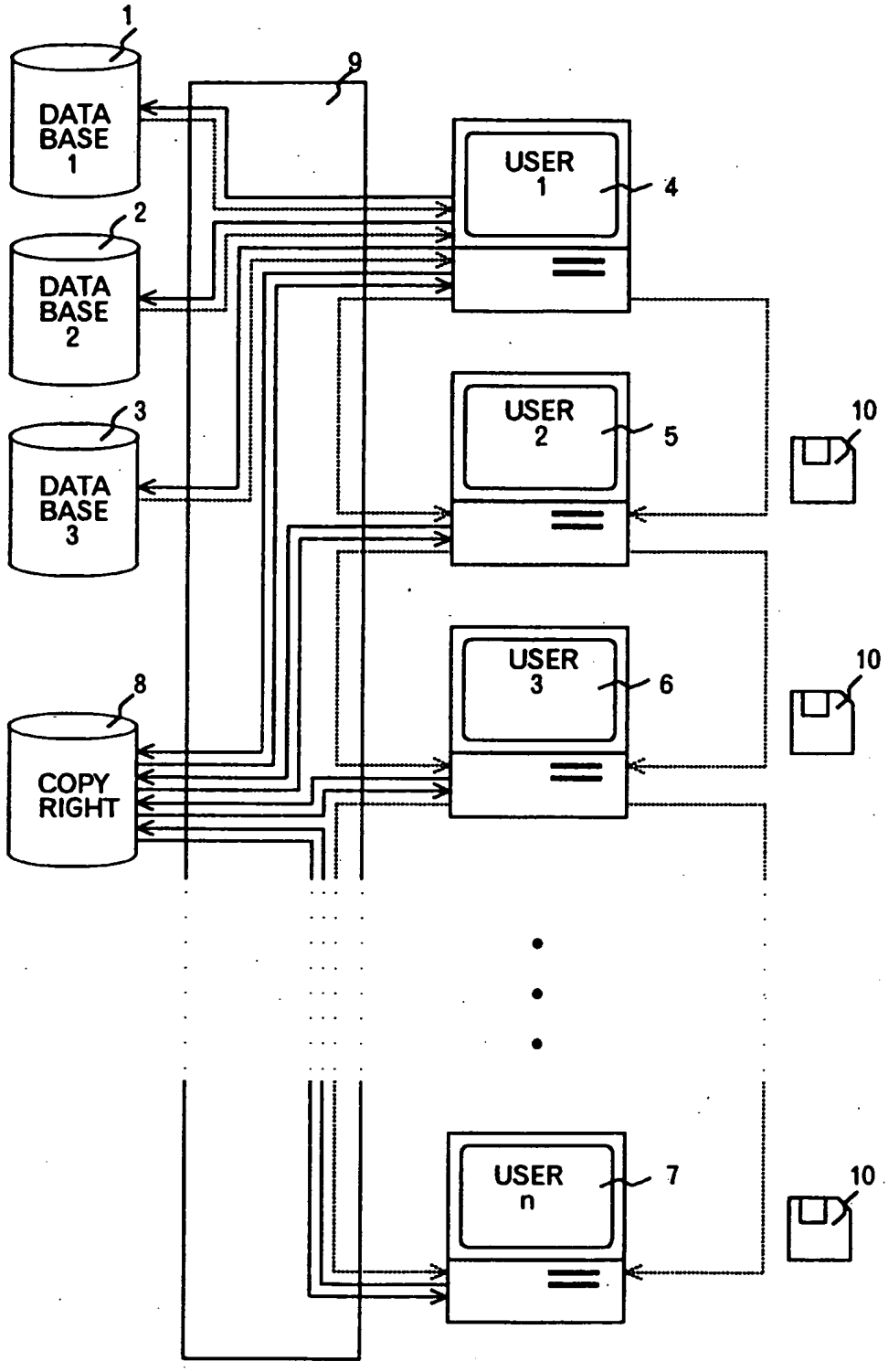

1
DATA BASE 1
2
DATA BASE 2
3
DATA BASE 3
8
COPY RIGHT
9
USER 1
4
USER 2
5
USER 3
6
USER n
7
10
10
10

Fig. 2

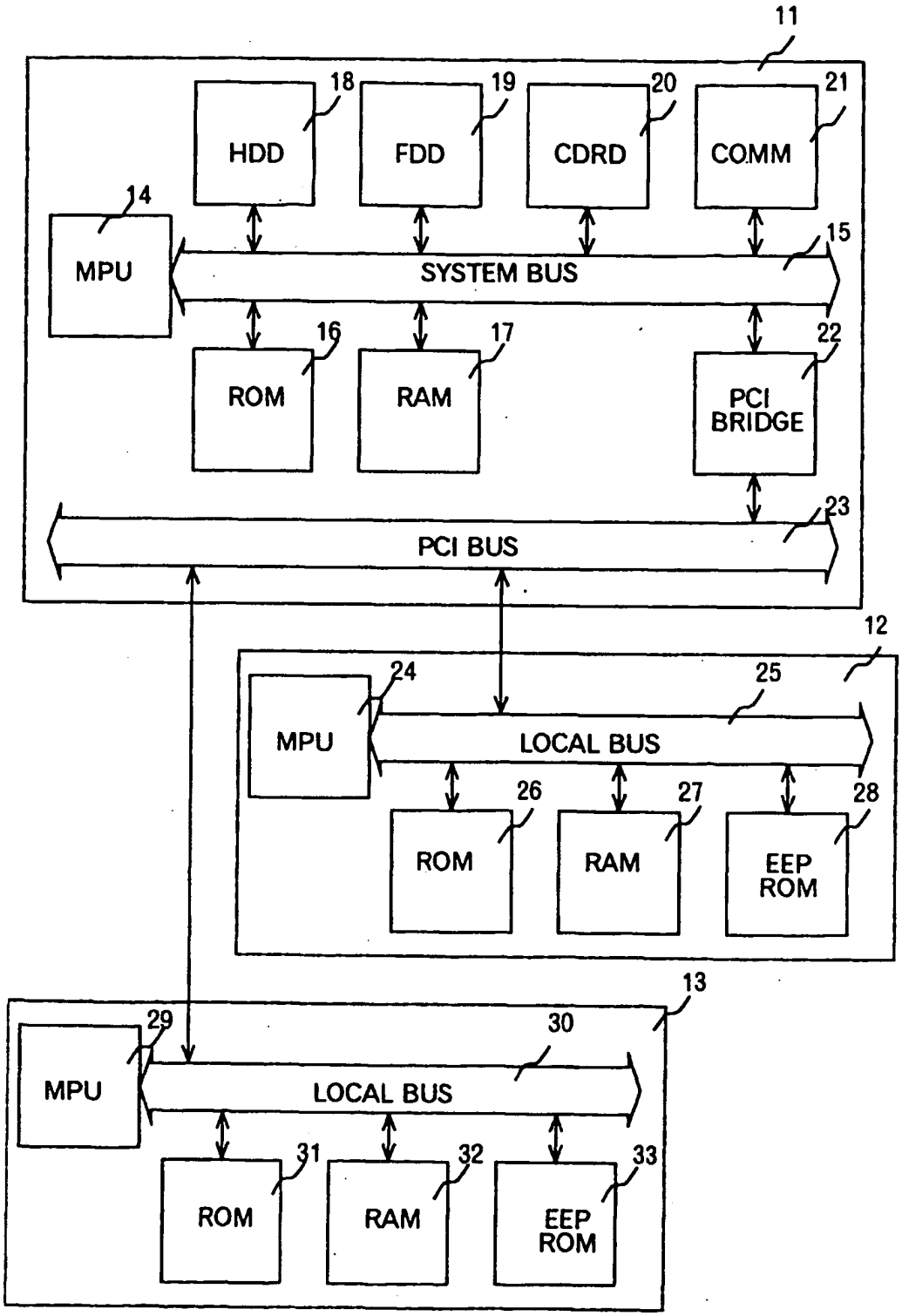

11
18
19
20
21
HDD
FDD
CDRD
COMM
14
MPU
15
SYSTEM BUS
16
17
22
ROM
RAM
PCI BRIDGE
23
PCI BUS
12
24
25
MPU
LOCAL BUS
26
27
28
ROM
RAM
EEP ROM
13
29
30
MPU
LOCAL BUS
31
32
33
ROM
RAM
EEP ROM

Fig. 3

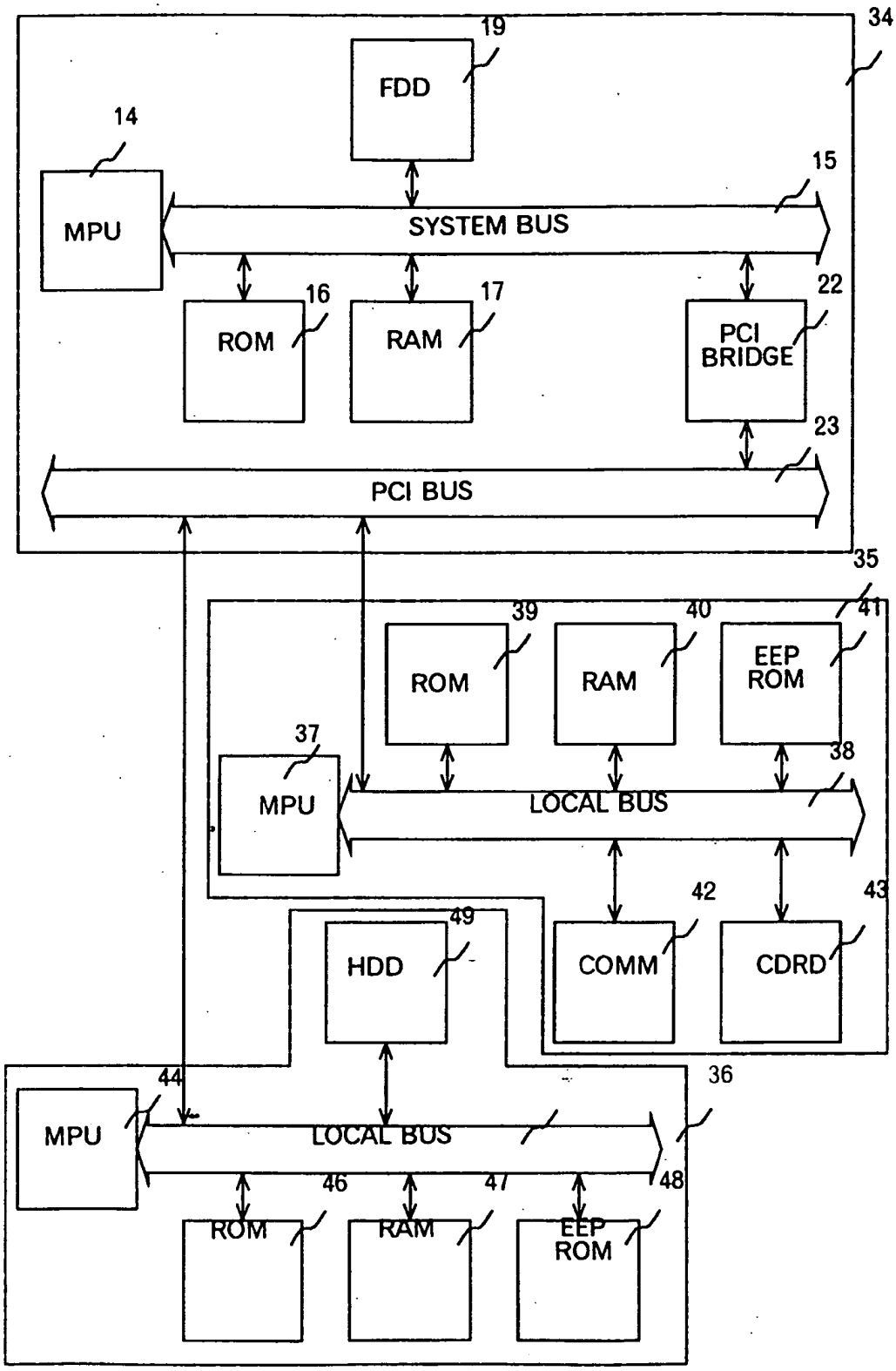

34
19
FDD
14
15
MPU
SYSTEM BUS
16
17
22
ROM
RAM
PCI BRIDGE
23
PCI BUS
35
39
40
41
ROM
RAM
EEP ROM
37
38
MPU
LOCAL BUS
42
43
49
HDD
COMM
CDRD
36
44
MPU
LOCAL BUS
46
47
48
ROM
RAM
EEP ROM

Fig. 4

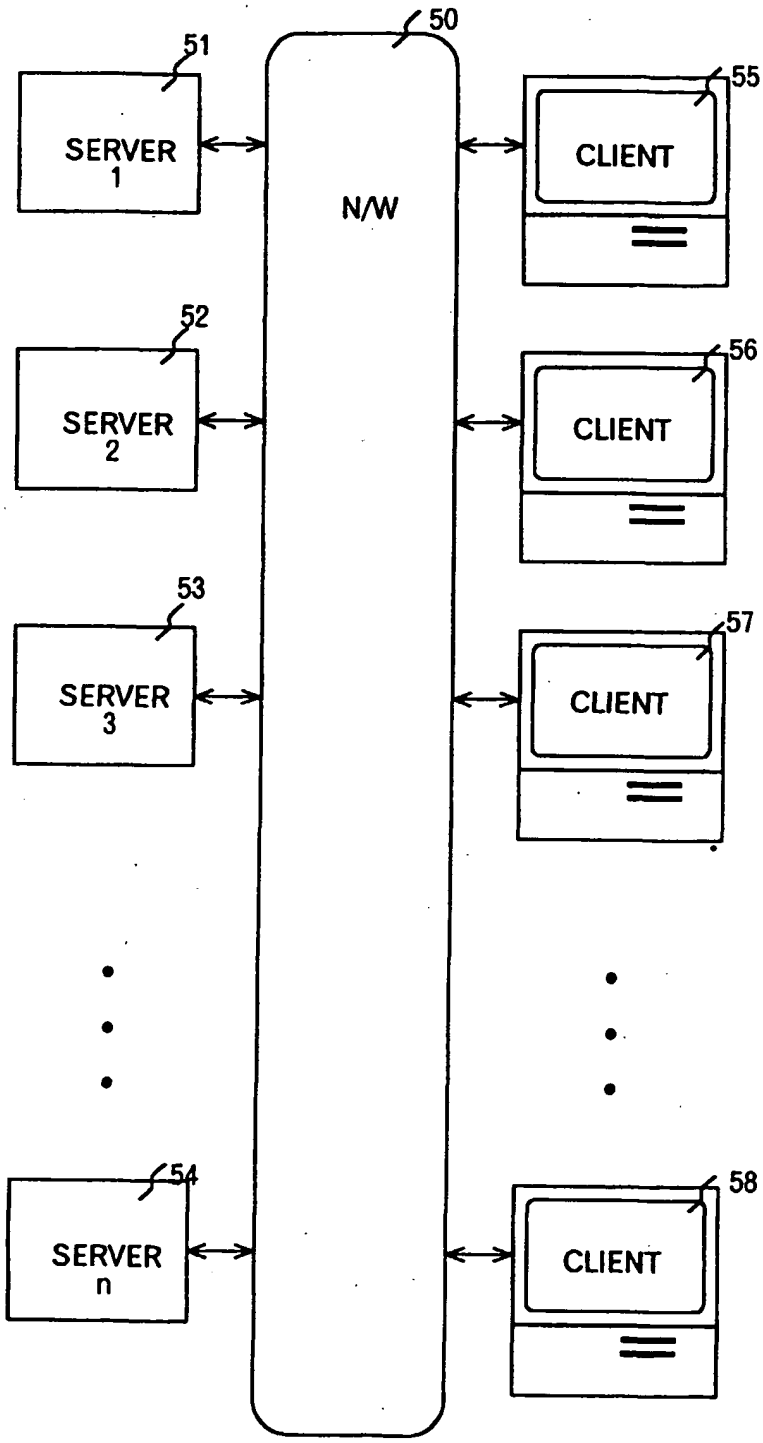
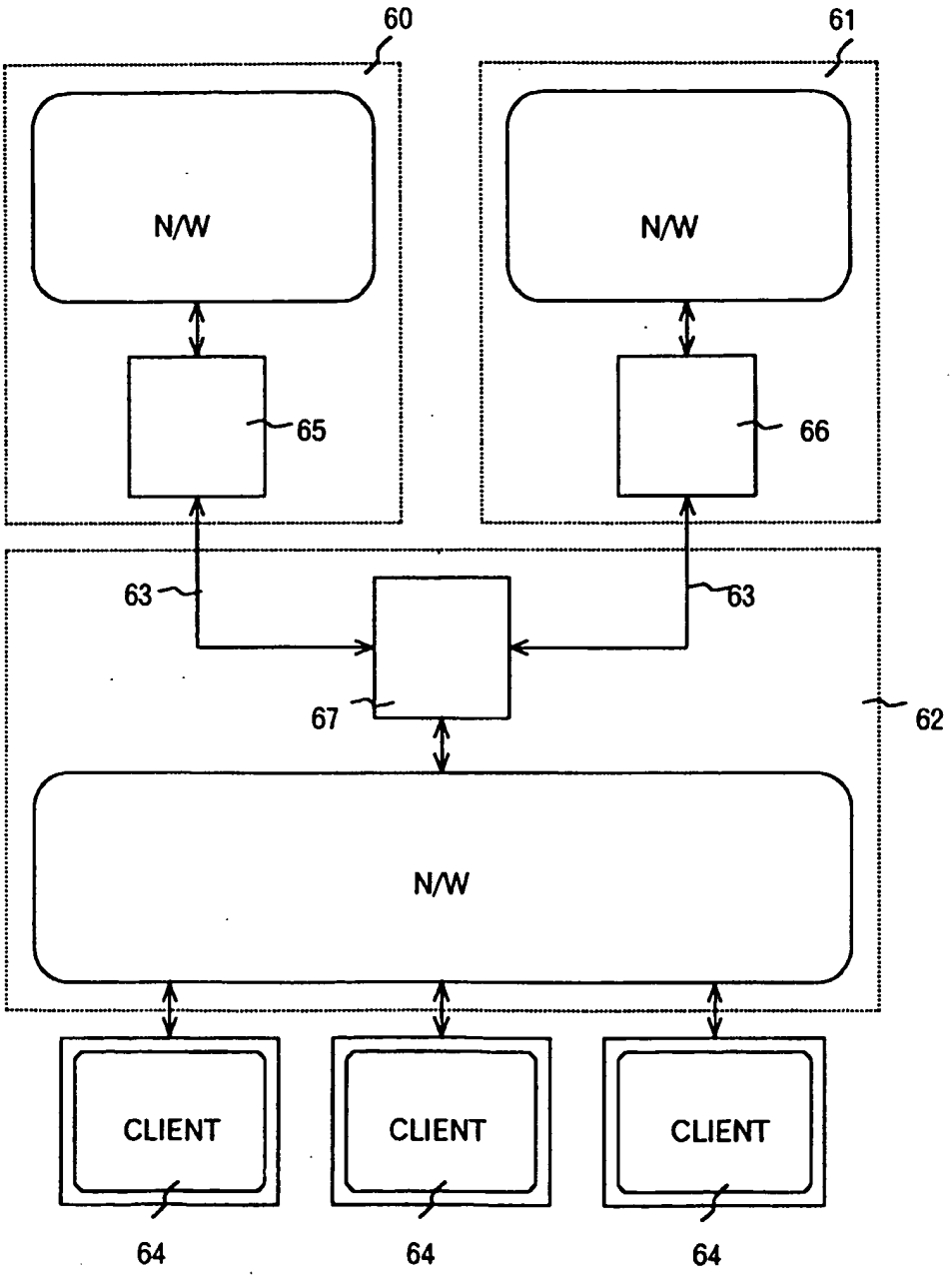

50
51
SERVER 1
N/W
55
CLIENT
52
SERVER 2
56
CLIENT
53
SERVER 3
57
CLIENT
54
SERVER n
58
CLIENT

Fig. 5



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 880 088 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
09.01.2002 Bulletin 2002/02

(43) Date of publication A2:
25.11.1998 Bulletin 1998/48

(21) Application number: **98109085.5**

(22) Date of filing: **19.05.1998**

(51) Int Cl.[7]: **G06F 1/00**, H04L 29/06

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **23.05.1997 JP 14999997**

(71) Applicant: **MITSUBISHI CORPORATION**
Chiyoda-ku, Tokyo 100-0005 (JP)

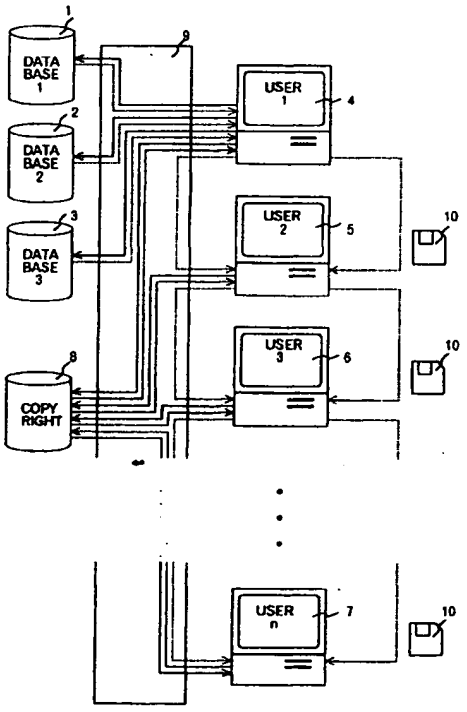
(72) Inventor: **Saito, Makoto**
Tama-shi (JP)

(74) Representative: **Neidl-Stippler, Cornelia, Dr.**
Rauchstrasse 2
81679 München (DE)

(54) Data copyright management system and apparatus

(57) There are provided a digital content management apparatus which further embodies a digital content management apparatus used with a user terminal, and a system which protects the secrets of a digital content. The system and the apparatus are a real time operating system using a micro-kernel, which is incorporated in the digital content management apparatus as an interruption process having high priority, or is arranged in a network system using the digital content. When a user uses the digital content, whether there is an illegitimate usage or not, is watched by interrupting the usage process. In the case where illegitimate usage is carried out, a warning is given or the usage is stopped. The decryption/re-encryption functions of the digital content management apparatus having the decryption/re-encryption functions are not restricted to the inside of the user apparatus. By providing the decryption/re-encryption functions between the networks, the exchange of secret information between different networks is secured. By using this apparatus for converting a crypt algorithm, information exchange is made possible between systems which adopt different algorithms.

Fig. 1



EP 0 880 088 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 10 9085

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	WO 96 23257 A (TANDEM COMPUTERS INC) 1 August 1996 (1996-08-01) * page 1, line 19 - page 2, line 3 * * page 3, line 16 - line 26 * * page 8, line 14 - line 32 * * figure 1 *	1	G06F1/00 H04L29/06
X	WO 96 13113 A (SECURE COMPUTING CORP) 2 May 1996 (1996-05-02) * abstract * * page 13, line 12 - line 24 * * page 47, line 26 - page 48, line 9 * * figures 2,3 *	3	
D,Y	EP 0 715 241 A (MITSUBISHI CORP) 5 June 1996 (1996-06-05) * abstract * * column 3, line 58 - column 4, line 23 * * column 12, line 53 - line 58 * * column 14, line 11 - line 35 * * column 25, line 21 - line 57 * * figures 1,3,11 *	2,4-8	
D,Y	EP 0 677 949 A (MITSUBISHI CORP) 18 October 1995 (1995-10-18) * column 2, line 47 - column 3, line 9 *	2,4-8	

-/--

TECHNICAL FIELDS SEARCHED (Int.Cl.6)
G06F
H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	7 November 2001	Arbutina, L

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

Application Number
EP 98 10 9085

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing more than ten claims.

☐ Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims and for those claims for which claims fees have been paid, namely claim(s):

☐ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

see sheet B

☒ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.

☐ As all searchable claims could be searched without effort justifying an additional fee, the Search Division did not invite payment of any additional fee.

☐ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:

☐ None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims:

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 10 9085

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	LENNIL P: "THE IBM MICROKERNEL TECHNOLOGY" OS/2 DEVELOPER, MILLER FREEMAN, SAN FRANCISCO, CA, US, vol. 5, no. 5, 1 November 1993 (1993-11-01), pages 70-72,74, XP000672962 ISSN: 1073-0729 * page 70, left-hand column, paragraph 1 - page 71, left-hand column, paragraph 1 * * page 74, right-hand column, paragraph 1 *	1,2,4	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	7 November 2001	Arbutina, L

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

LACK OF UNITY OF INVENTION
SHEET B

Application Number
EP 98 10 9085

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. Claims: 1,2,4-8

   Managing digital content copyrights in a network by using real time watch program

2. Claim : 3

   Protecting secrets of a digital content in a network by using encryption/re-encryption between networks

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 10 9085

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

07-11-2001

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9623257 A	01-08-1996	CA 2210494 A1	01-08-1996
		EP 0806009 A1	12-11-1997
		JP 11504141 T	06-04-1999
		WO 9623257 A1	01-08-1996
WO 9613113 A	02-05-1996	US 5864683 A	26-01-1999
		AU 3888595 A	15-05-1996
		DE 69522460 D1	04-10-2001
		EP 0787397 A1	06-08-1997
		WO 9613113 A1	02-05-1996
EP 0715241 A	05-06-1996	EP 0715241 A2	05-06-1996
		JP 8287014 A	01-11-1996
		US 2001013021 A1	09-08-2001
		US 5867579 A	02-02-1999
		US 6128605 A	03-10-2000
EP 0677949 A	18-10-1995	JP 7271865 A	20-10-1995
		EP 1133163 A2	12-09-2001
		EP 0677949 A2	18-10-1995

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82